REMARKS

The Office Action mailed April 2, 2007 has been reviewed and the comments of the Patent and Trademark Office have been considered. Claims 1-14 were pending in the application. Claims 1, 8, 10, 11, 13 and 14 have been amended. A detailed listing of all claims that are, or were, in the application, irrespective of whether the claim(s) remain under examination in the application, are presented, with an appropriate defined status identifier. Thus, claims 1-14 remain pending in the application.

Claim Objections

Claim 13 is objected to because of an informality. The claim has been amended to address this issue. Reconsideration and withdrawal of this objection is respectfully requested.

Claims 8, 10, 11 and 14 are objected to because of informalities. The claims have been amended to address this issue. Reconsideration and withdrawal of this objection is respectfully requested.

Specification Objections

The specification is objected to because it contains an embedded hyperlink. The specification has been amended to address this issue. Reconsideration and withdrawal of this objection is respectfully requested.

Prior Art Rejections

Claims 1-9 and 13 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 7,039,803 to Lotspiech (hereinafter "Lotspiech") in view of U.S. Patent Application Publication 2002/0029337 to Sudia (hereinafter "Sudia"). Claims 10-12 and 14 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Sudia in view of Lotspiech. Applicant respectfully traverses these rejections for at least the following reasons.

The present invention relates to the distribution of cryptographic keys which are generated from an ancestral hierarchy. Such keys are often used to protect access to subscription services, for example. The manner in which the keys are generated means that, once one key is invalidated or compromised, it effectively compromises the security of other keys within the hierarchy - at least to the extent that a common ancestry with the invalidated or compromised key is shared. Invalidation or compromise of keys can, therefore, require reissue of keys more widely, which is an expensive business.

-6-

The invention lies in a realization that optimizes the commercial value of the key hierarchy. Specifically, users of the service are grouped within the ancestral hierarchy so that, for example, similar value and/or behavior users share close ancestry. This enables, for example, 'disruptive' users - e.g. those who are likely either to unsubscribe or behave in another way that might invalidate or compromise related keys - to be kept as far apart in the hierarchy as possible from the higher value, more reliable users. The result may be, therefore, that low value, disruptive users may experience the inconvenience of key reissue more frequently, precisely as a result of the disruptive behavior of a member of that group, while the higher value, more stable users do not experience that inconvenience as often. Further, because one part of the hierarchy is kept for low value users, decisions may be taken to ignore invalidation in the low value user group - with only limited loss of revenue from that group as a result of illegal decryption (due to the low value at risk) as well as only a relatively low likelihood of compromise of the higher value services due to the distinct positioning of groups within the cryptographic hierarchy.

As mentioned above, the Examiner rejects the claims under 35 U.S.C. § 103(a), combining Lotspiech and Sudia. Lotspiech appears generally relevant to cryptographic keys generated from an ancestral hierarchy. Sudia is related to digital signatures. The Examiner contends this to be an 'analogous art'. However, digital signatures and cryptographic keys are two very different things which, perhaps most pertinently, serve two very different purposes: keys protect and restrict access; whereas signature authenticate. Thus, it is respectfully submitted that this combination would not occur to one of ordinary skill in the art of encryption and thus is not proper.

Thus, when the Examiner cites to paragraphs 46 - 50 of Sudia, where a hierarchical structure is proposed for certificates which reflects the organizational structure of a sponsor organization, this is not applicable to cryptographic keys in the way which is inferred in the rejection.

First of all, the structure reflected in the hierarchical structure of the signatures is that of the sponsor organization, rather than a consequence of any cryptographic process of generation. The independent claims requires that users are grouped within the key hierarchy.

-7-

However, in the teachings of Sudia, the key hierarchy is being generated to reflect the user groups. Thus, applying Sudia's teaching - assuming for the sake of argument that it could technically be combined in the way suggested - doesn't actually combine with Lotspiech to teach the invention.

Secondly, the signatures in Sudia have the purpose of authenticating provenance. All signatures authenticate provenance from within a single organization. It follows that, if there is compromise of a signature to someone else within the organization, the consequences won't be grave because all signature holders are, legally at least, 'on the same side' - because they're all part of the same organization. That is a marked contrast to the instant invention, in which keys issued on behalf of a service provider, for example, whose function is to restrict access to the services. In the latter claimed situation, the key issuer is the single body and the key users are members of the public who have no legal obligation to 'be on the same side'. Nor indeed, in practice are those members of the public 'on the same side' as the issuer, so the real possibility exists that a compromised key may be used to gain illegal access to information or services. Both of these differences, and particularly the second one, is founded in the fundamental difference between keys on the one hand and signatures on the other.

The independent claims reflect these points, asserting that the allocation of a distinct domain within the hierarchy occurs for each group of users, and further that the keys are issued on behalf of an organization providing the service to which access is restricted and to would-be users of the service. In contrast, Sudia teaches that the certificates utilized to authorize access reflects the structure of a sponsor organization. (paragraph 0047) Thus, the structure reflected in the hierarchical structure of the signatures is the structure of the sponsor organization, instead of a structure created from a cryptographic process of generation. Consequently, the domains for each group of users within the hierarchy based upon characteristics of access of the groups are not created in Sudia. The hierarchy mirrors the structure of the organization rather than supporting the varied access characteristics of different groups of users in a domain. Thus, the combination of Lotspiech with Sudia fails to teach these features as claimed in the independent claims.

The dependent claims that depend from the independent claims are also patentable for at least the same reasons as the independent claims on which they ultimately depend. In addition, they recite additional patentable features when considered as a <u>whole</u>. As mentioned above, Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 C.F.R. § 1.25. Additionally, charge any fees to Deposit Account 08-2025 under 37 C.F.R. § 1.16 through § 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Respectfully submitted,

Date June 1, 2007

By _L. K_____, Reg. No. 59,396_

Customer Number: 22879
Telephone: (202) 672-5485
Facsimile: (202) 672-5399

William T. Ellis
Attorney for Applicant
Registration No. 26,874

-9-